

New Semifield Planes of order 81^{*}

I.F. Rúa[†]Elías F. Combarro[‡]

Abstract

A finite semifield D is a finite nonassociative ring with identity such that the set $D^* = D \setminus \{0\}$ is closed under the product. From any finite semifield a projective plane can be constructed. In this paper we obtain new semifield planes of order 81 by means of computational methods. These computer-assisted results yield to a complete classification (up to isotopy) of 81-element finite semifields.

1 Introduction

A **finite semifield** (or finite division ring) D is a finite nonassociative ring with identity such that the set $D^* = D \setminus \{0\}$ is closed under the product, i.e., it is a loop [1, 2]. Finite semifields have been traditionally considered in the context of finite geometries since they coordinatize projective semifield planes [3]. Recent applications to coding theory [4, 5, 6], combinatorics and graph theory [7], have broaden the potential interest in these rings.

Because of their diversity, the obtention of general theoretical algebraic results seems to be a rather difficult (and challenging) task. On the other hand, because of their finiteness, computational methods can be naturally considered in the study of these objects. So, the classification of finite semifields of a given order is a rather natural problem to use computations. For instance, computers were used in the classification up to isotopy of finite semifields of order 32 [8, 1]. This computer-assisted classification is equivalent to the classification of the corresponding projective semifield planes up to isomorphism [9].

In this paper we obtain a classification up to isotopy of finite semifields with **81 elements**. It turns out that approximately one half of the 81-element semifield planes were previously unknown.

The structure of the paper is as follows. In §2, basic properties of finite semifields are reviewed. Finally, in §3, a complete description of 81-element finite semifields is given.

^{*}This is a revised paper (original title: *New semifield planes of orders 64 and 81*). During the referee process the authors were informed that U. Dempwolff had previously and independently obtained a classification of finite semifields of order 81 (*Semifield Planes of Order 81*, J. of Geometry (to appear)). So, the current version (unpublished) contains only the results concerning 81 element finite semifields. For the results on order 64 the reader is referred to *Classification on 64-element finite semifields* (I.F. Rúa, E.F. Combarro and J. Ranilla) arXiv:0807.2994v1

[†]Departamento de Matemáticas, Universidad de Oviedo, rua@uniovi.es . Partially supported by FICYT (IB05-186) and MEC - MTM - 2007 - 67884 C04 - 01

[‡]Departamento de Informática, Universidad de Oviedo, elias@aic.uniovi.es . Partially supported by MEC -TIN - 2007 - 61273

2 Preliminaries

In this section we collect definitions and facts on finite semifields. Proofs of these results can be found, for instance, in [1, 2].

Definition 1. A finite nonassociative ring D is called **presemifield**, if the set of nonzero elements D^* is closed under the product. If D has an identity element, then it is called **finite semifield**.

If D is a finite semifield, then D^* is a multiplicative loop. That is, there exists an element $e \in D^*$ (the identity of D) such that $ex = xe = x$, for all $x \in D$ and, for all $a, b \in D^*$, the equation $ax = b$ (resp. $xa = b$) has a unique solution.

Besides finite fields (which are obviously finite semifields), finite semifields were first considered by L.E. Dickson [10] and were deeply studied by A.A. Albert [11, 12, 9, 13]. The term “finite semifield” was introduced in 1965 by D.E. Knuth [1]. These rings play an important role in the study of certain projective planes, called *semifield planes* [3, 1]. Recently, applications of finite semifields to coding theory have been also considered [4, 5, 6]. Also, connections to combinatorics and graph theory have been found [7].

Proposition 1. *The characteristic of a finite presemifield D is a prime number p , and D is a finite-dimensional algebra over $GF(q)$ ($q = p^c$) of dimension d , for some $c, d \in \mathbb{N}$, so that $|D| = q^d$. If D is a finite semifield, then $GF(q)$ can be chosen to be its associative-commutative center $Z(D)$.*

Definition 2. A finite semifield D is called **proper**, if it is not associative.

Because of Wedderburn’s theorem [14], finite semifields are either proper or finite fields. The existence of proper semifields is guaranteed by the following result.

Theorem 1. *If D is a proper semifield of dimension d over $Z(D)$, then $d \geq 3$ and $|D| \geq 16$. Moreover, for any prime power $p^n \geq 16$, with $n \geq 3$, there exists a proper semifield D of cardinality p^n .*

The definition of isomorphism of presemifields is the usual one for algebras, and classification of finite semifields up to isomorphism can be naturally considered. Because of the connections to finite geometries, we must also consider the following notion.

Definition 3. If D_1, D_2 are two presemifields, then an **isotopy** between D_1 and D_2 is a triple (F, G, H) of bijective linear maps $D_1 \rightarrow D_2$ such that

$$H(ab) = F(a)G(b) \quad \forall a, b \in D_1.$$

It is clear that any isomorphism between two presemifields is an isotopy, but the converse is not necessarily true. It can be shown that any presemifield is isotopic to a finite semifield [1, Theorem 4.5.4]. From any presemifield D a projective plane $\mathcal{P}(D)$ can be constructed (see [3, 1] for the details of this construction). Theorem 6 in [9] shows that isotopy of finite semifields is the algebraic translation of the isomorphism between the corresponding projective

planes. So, two finite semifields D_1, D_2 are isotopic if, and only if, the projective planes $\mathcal{P}(D_1), \mathcal{P}(D_2)$ are isomorphic. The set of isotopies between a finite semifield and itself is a group under composition, called the **autotopy** group.

Given a finite semifield D , it is possible to construct the set \mathcal{D} of all its isotopic but non necessarily isomorphic finite semifields. It can be obtained from the **principal isotopes** of D [1]. A principal isotope of D is a finite semifield $D_{(y,z)}$ (where $y, z \in D^*$) such that $(D_{(y,z)}, +) = (D, +)$ and multiplication is given by the rule

$$a \cdot b = R_z^{-1}(a)L_y^{-1}(b) \quad \forall a, b \in D$$

where $R_z, L_y : D \rightarrow D$ are the maps $R_z(a) = az, L_y(a) = ya$, for all $a \in D$. Moreover, there is a relation between the order of $\text{At}(D)$, the autotopy group of D , and the orders of the automorphism groups of the elements in \mathcal{D} [1, Theorem 3.3.4].

Theorem 2. *If D is a finite semifield, and \mathcal{D} is the set of all nonisomorphic semifields isotopic to D , then*

$$(|D| - 1)^2 = |\text{At}(D)| \sum_{E \in \mathcal{D}} \frac{1}{|\text{Aut}(E)|}$$

The sum of the right term will be called the Semifield/Automorphism (S/A) sum.

If $\mathcal{B} = [x_1, \dots, x_d]$ is a $GF(q)$ -basis of a presemifield D , then there exists a unique set of constants $\mathbf{A}_{D,\mathcal{B}} = \{A_{i_1 i_2 i_3}\}_{i_1, i_2, i_3=1}^d \subseteq GF(q)$ such that

$$x_{i_1} x_{i_2} = \sum_{i_3=1}^d A_{i_1 i_2 i_3} x_{i_3} \quad \forall i_1, i_2 \in \{1, \dots, d\}$$

It is called **3-cube** corresponding to D with respect to the basis \mathcal{B} [1]. This set is also known as multiplication table, and it completely determines the multiplication in D . If \mathcal{B}' is a second basis of D (where $\mathcal{B}' = \mathcal{B}P^t$, with $P \in \text{GL}(d, q)$), then the relation between the 3-cubes $\mathbf{A}_{D,\mathcal{B}}, \mathbf{A}_{D,\mathcal{B}'}$ is

$$\mathbf{A}_{D,\mathcal{B}'} = [P, P, P^{-t}] \times \mathbf{A}_{D,\mathcal{B}}$$

where $-t$ denotes inverse transpose, and

$$([F^1, F^2, F^3] \times \mathbf{A}_{D,\mathcal{B}})_{i_1 i_2 i_3} = \sum_{x_1, x_2, x_3=1}^d F_{i_1 x_1}^1 F_{i_2 x_2}^2 F_{i_3 x_3}^3 A_{x_1 x_2 x_3}$$

for all $F^1, F^2, F^3 \in \text{GL}(d, q)$ [1, (4.11)].

A remarkable fact is that permutation of the indexes of a 3-cube preserves the absence of nonzero divisors. Namely, if D is a presemifield, and $\sigma \in S_3$ (the symmetric group on the set $\{1, 2, 3\}$), then the set

$$\mathbf{A}_{D,\mathcal{B}}^\sigma = \{A_{i_{\sigma(1)} i_{\sigma(2)} i_{\sigma(3)}}\}_{i_1, i_2, i_3=1}^d \subseteq GF(q)$$

is the 3-cube of a $GF(q)$ -algebra $D_{\mathcal{B}}^\sigma$ which has not zero divisors [1, Theorem 4.3.1]. Notice that, in general, different bases $\mathcal{B}, \mathcal{B}'$ lead to nonisomorphic presemifields $D_{\mathcal{B}}^\sigma, D_{\mathcal{B}'}^\sigma$. However, these presemifields are always isotopic. This is a consequence of the following two propositions.

Proposition 2. [1, Theorem 4.4.2] Let D_1, D_2 be two presemifields of dimension d over a finite field $GF(q)$, and let $\mathcal{B}_1, \mathcal{B}_2$ be two $GF(q)$ -bases of D_1 and D_2 . Then, D_1 and D_2 are isotopic if and only if there exist three nonsingular maps $F^1, F^2, F^3 \in GL(d, q)$ such that $\mathbf{A}_{D_2, \mathcal{B}_2} = [F^1, F^2, F^3] \times \mathbf{A}_{D_1, \mathcal{B}_1}$.

Proposition 3. [1, Theorem 4.2.3] Let D be a presemifield of dimension d over $GF(q)$, and let \mathcal{B} be a $GF(q)$ -basis of D . Then, for all $\sigma \in S_3$, and for all $F^1, F^2, F^3 \in GL(d, q)$,

$$([F^1, F^2, F^3] \times \mathbf{A}_{D, \mathcal{B}})^\sigma = [F^{\sigma^{-1}(1)}, F^{\sigma^{-1}(2)}, F^{\sigma^{-1}(3)}] \times \mathbf{A}_{D, \mathcal{B}}^\sigma$$

The number of projective planes that can be constructed from a given finite semifield D using the transformation of the group S_3 is at most six [1, Theorem 5.2.1]. Actually, S_3 acts on the set of semifield planes of a given order. So, the classification of finite semifields can be reduced to the classification of the corresponding projective planes up to isotopy and, ultimately, this can be reduced to the classification of semifield planes up to the action of the group S_3 . In this setting, we will consider a plane as *new* when no *known*¹ finite semifield coordinatizes a plane in its S_3 -orbit.

Invariance under the transformation by S_3 leads to the following definition.

Definition 4. Let D be a finite presemifield d -dimensional over $GF(q)$, and let $\sigma \in S_3$. Then, D is called:

- **σ -invariant**, if there exists a $GF(q)$ -basis \mathcal{B} of D , such that $\mathbf{A}_{D, \mathcal{B}}^\sigma = \mathbf{A}_{D, \mathcal{B}}$.
- **σ -isotopic**, if there exists a $GF(q)$ -basis \mathcal{B} of D , such that $D_{\mathcal{B}}^\sigma$ is isotopic to D .

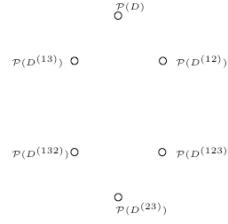
Clearly, if a presemifield is σ -invariant, then it is σ -isotopic. Different well-known notions can be rephrased in terms of this definition.

Example 1. A finite presemifield:

- Is commutative iff it is (1, 2)-invariant.
- Is symplectic [5] iff it is (1, 3)-invariant.
- Induces a self-dual plane [1] iff it is (1, 2)-isotopic.
- Induces a self-transpose plane [15] iff it is (1, 3)-isotopic.

It is clear that, if D is σ -invariant ($\mathbf{A}_{D, \mathcal{B}}^\sigma = \mathbf{A}_{D, \mathcal{B}}$, where \mathcal{B} is a $GF(q)$ -basis of D), then $\mathbf{A}_{D, \mathcal{B}}^{\sigma\tau} = \mathbf{A}_{D, \mathcal{B}}^\tau$, for all $\tau \in S_3$. Similarly, as a consequence of Proposition 3, if D is σ -isotopic (i.e., $D_{\mathcal{B}}^\sigma$ is an isotope of $D_{\mathcal{B}}$, where \mathcal{B} is a $GF(q)$ -basis of D), then $D_{\mathcal{B}}^{\sigma\tau}$ is an isotope of $D_{\mathcal{B}}^\tau$. This fact will be useful in the description of all possible situations depending on the orbits of S_3 (cf. [15, Proposition 3.8], [1, Corollary 5.2.2]). We shall use a graphical representation to distinguish between the different cases. The vertices of an hexagon will depict the six different planes obtained from a given finite semifield (cf. [1, Theorem 5.2.1]).

¹We have considered as *known* semifields those appearing in the, up to our knowledge, last survey on the topic, [19]



A dotted line between two planes shows that the corresponding finite semifields are σ -isotopic (where σ is a suitable element of S_3). A continuous line stands for σ -invariance of one of the corresponding coordinatizing finite presemifields. Here are the different possibilities (cf. [1, Corollary 5.2.2],[15, Proposition 3.8]).

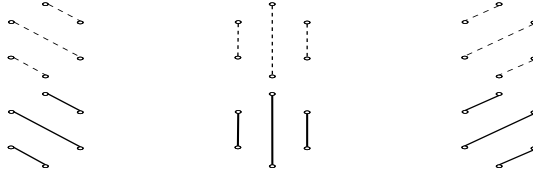
- A unique orbit consisting of six planes.



- Two orbits of three planes each.



- Three orbits of two planes each.



- Six different planes.



We finish this section recalling that the construction of finite semifields of a given order can be rephrased as a matrix problem [16, Proposition 3].

Proposition 4. *There exists a finite semifield D of dimension d over its center $Z(D) \supseteq GF(q)$ if, and only if, there exists a set of d matrices $\{A_1, \dots, A_d\} \subseteq GL(d, q)$ such that:*

1. A_1 is the identity matrix;
2. $\sum_{i=1}^d \lambda_i A_i \in GL(d, q)$, for all **non-zero tuples** $(\lambda_1, \dots, \lambda_d) \in \prod^d GF(q)$, that is, $(\lambda_1, \dots, \lambda_d) \neq \vec{0}$.
3. The first column of the matrix A_i is the column vector e_i^\perp with a 1 in the i -th position, and 0 everywhere else.

3 New Semifield Planes of order 81: a classification

This section is devoted to the study of semifield planes of order 81. All these planes have been obtained by exhaustive search of coordinatizing semifields, and a complete classification has been later achieved.

Let us begin by fixing some notation. If D is a finite semifield with 81 elements, then it is a finite nonassociative algebra of dimension 4 over \mathbb{Z}_3 . From [16][Proposition 3] there exists a set of matrices $\{A_1 = I_4, A_2, A_3, A_4\} \subseteq GL(4, 3)$ with the first column of A_i equal to the vector e_i^\perp ($i = 1, \dots, 4$), such that $\sum_{i=1}^4 \lambda_i A_i \in GL(4, 3)$, for all non-zero tuples $(\lambda_1, \lambda_2, \lambda_3, \lambda_4) \in \prod_{i=1}^4 \mathbb{Z}_3$. These matrices are the coordinate matrices of the maps R_{x_i} where $\mathcal{B} = \{x_1 = e, x_2, x_3, x_4\}$ is a \mathbb{Z}_3 -basis of D . Hence, the existence of 81-element semifields is reduced to the existence of sets of 4 matrices satisfying certain conditions. The first of these matrices is always the identity matrix. Let us now show that the second matrix can also be chosen from a small amount of matrices.

Proposition 5. *If D is a finite semifield with 81 elements, then there is a \mathbb{Z}_3 -basis $\mathcal{B} = \{x_1 = e, x_2, x_3, x_4\}$ of D such that the coordinate matrix of R_{x_2} is a companion matrix of one of the following polynomials:*

- (1) $x^4 + x + 2$ (2) $x^4 + 2x + 2$ (3) $x^4 + x^3 + 2$
- (4) $x^4 + x^3 + x^2 + 2x + 2$ (5) $x^4 + x^3 + 2x^2 + 2x + 2$ (6) $x^4 + 2x^3 + 2$
- (7) $x^4 + 2x^3 + x^2 + x + 2$ (8) $x^4 + 2x^3 + 2x^2 + x + 2$

Proof. From [16][Theorem 2] the finite semifield D is left and right primitive [17]. Therefore, there exists an element $x_2 \in D$ such that the characteristic polynomial $p_{x_2}(x)$ of the linear transformation R_{x_2} is a primitive polynomial of degree 4 over \mathbb{Z}_3 [16][Proposition 2]. So, in view of the list of the primitive polynomials of order 4 over \mathbb{Z}_3 [18] it must be one of the eight listed above. Moreover, in particular, $p_{x_2}(z)$ is irreducible in $\mathbb{Z}_3[z]$, and so $\mathcal{B} = \{1, x_2, x_2^2, x_2^3\}$ is a linearly independent set, i.e., it is a \mathbb{Z}_3 -basis of D . The coordinate matrix of R_{x_2} with respect to such a basis is clearly a companion matrix. \square

We have used this property to design a search algorithm for 81-element finite semifields. Our algorithm, which is a rather standard backtracking method (cf. [8]), is written below with the help of two auxiliary functions. The first one (*Complete*) enumerates all valid semifields with given initial matrices. The second one (*Complete2*) enumerates all valid semifield with given initial matrices and some columns of the next matrix. The function *Complete* uses the already known matrices to create the initial columns of the next matrix and then calls *Complete2*. This second function, in turn, recursively adds columns to the incomplete matrix (backtracking if necessary) and then calls *Complete* with new matrix.

Algorithm 1: Search algorithm for finite semifields

• **Input:** Characteristic p and dimension n of the semifields, second matrix A_2

- **Output:** List of matrices representing all the semifields with second matrix A_2 , of the given characteristic and dimension
 - **Procedure:**
 - Create an empty list of matrices L
 - Insert the identity I in L
 - Insert A_2 in L
 - Call $Complete(L, p, n)$
-

Algorithm 2: Function *Complete*

- **Input:** A list of matrices L , the characteristic p and the dimension n
 - **Output:** List of matrices representing all the semifields with initial matrices L , of the given characteristic and dimension
 - **Procedure:**
 - $m \leftarrow \text{size of } L$
 - if** m is equal to n **then**
 - return** L
 - end**
 - else**
 - Create a matrix M of 1 column
 - Set the first column of M equal to the $(m+1)$ -th column of the identity
 - Call $Complete2(L, M, p, n)$
 - end**
-

Algorithm 3: Function *Complete2*

- **Input:** A list of matrices L , a truncated matrix M , the characteristic p and the dimension n
- **Output:** List of matrices representing all the semifields with initial matrices L and M , of the given characteristic and dimension
- **Procedure:**
 - $k \leftarrow \text{number of columns of } M$
 - if** k is equal to n **then**
 - Insert M in L
 - Call $Complete(L, p, n)$
 - end**
 - else**
 - Compute C , the list of columns c such that the join of M and c is linearly independent of the matrices of L (truncated at the $k+1$ first columns)
 - for** each c in C **do**
 - Join c to M , as its $k+1$ -th column
 - Call $Complete2(L, M, p, n)$
 - Remove c from M
 - end**
 - end**

We have implemented this algorithm in the language C++. The run time on a 2GHz desktop computer was about 150 seconds (for each separate case). As output, the following number of tuples were obtained:

Form of A_2	Number of tuples (A_3, A_4, A_5, A_6)
(1)	6811
(2)	6811
(3)	6811
(4)	7866
(5)	7866
(6)	6811
(7)	7866
(8)	7866

These tuples were later processed by a classification algorithm.

Algorithm 4: Isomorphism classification algorithm

- **Input:** A collection of lists of matrices representing semifields
 - **Output:** Representatives of all isomorphism classes present in the collection
 - **Procedure:**

```

 $S \leftarrow \emptyset$ 
for each list  $L$  of matrices in the collection do
  if  $L \notin S$  then
    print  $L$ 
    Insert in  $S$  all cyclic representations of  $L$ 
  end
end

```
-

The correctness of the algorithm is guaranteed by [16][Theorem 2], since any primitive semifield is necessarily cyclic. The algorithm produced 2826 isomorphism classes that were later processed by another algorithm which classified semifields under isotopy and S_3 -action. The output of this third algorithm showed the existence of 27 isotopy classes and 12 different planes (up to S_3 -equivalence).

Algorithm 5: Isotopy and S_3 -action classification algorithm

- **Input:** A collection of lists of matrices representing semifields
- **Output:** Representatives of all isotopy and S_3 -action classes present in the collection
- **Procedure:**

```

 $S \leftarrow \emptyset$ 
for each list  $L$  of matrices in the collection do
  if  $L \notin S$  then
    print  $L$ 
     $T \leftarrow \emptyset$ 

```



```

    if classification is under  $S_3$ -action then
      for each  $\sigma$  in  $S_3$  do
        Insert  $\sigma(L)$  in  $T$ 
      end
    else
      Insert  $L$  in  $T$ 
    end
    for each  $I$  in  $T$  do
      for each principal isotope  $J$  of  $I$  do
        Insert in  $S$  all cyclic representations of  $J$ 
      end
    end
  end
end
end

```

At this point we obtained a complete classification of the known semifield planes of order 81. We explicitly constructed all finite semifields of such an order that belong to any of the families collected in [19]. Classification under isomorphism, isotopy and S_3 -action showed the existence of 7 known planes (up to S_3 -action), that we list below. As before, a semifield representative is given for each plane, together with the order of its automorphism group (for a detailed description of the constructions, see [19]).

I (Desarguesian plane)

Finite field $\text{GF}(81)$ (4 automorphisms)

$$(A_2, A_3, A_4) = (19792, 8866, 186745)$$

II (Twisted field plane)

Twisted Field (1 automorphism) with parameters:

- $j \in \text{GF}(81)$ such that $j^4 + 2j + 2 = 0$;
- $\alpha \in \text{Aut}(\text{GF}(81))$ such that $\alpha(x) = x^3$, for all $x \in \text{GF}(81)$;
- $\beta \in \text{Aut}(\text{GF}(81))$ such that $\beta(x) = x^{3^3}$, for all $x \in \text{GF}(81)$.

$$(A_2, A_3, A_4) = (19792, 30332, 214473)$$

III (Commutative semifield)

Dickson's commutative semifield (4 automorphisms) with parameters:

- $k \in \text{GF}(9)$ such that $k^2 + 2k + 2 = 0$;
- $\sigma \in \text{Aut}(\text{GF}(9))$ such that $\sigma(x) = x^3$, for all $x \in \text{GF}(9)$.

$$(A_2, A_3, A_4) = (19818, 9001, 355161)$$

IV

Knuth's semifield of type 1 (8 automorphisms) with parameters:

- $k \in \text{GF}(9)$ such that $k^2 + 1 = 0$;
- $\alpha \in \text{Aut}(\text{GF}(9))$ such that $\alpha(x) = x^3$, for all $x \in \text{GF}(9)$.

- $\beta \in \text{Aut}(\text{GF}(9))$ such that $\beta(x) = x$, for all $x \in \text{GF}(9)$.
- $\gamma \in \text{Aut}(\text{GF}(9))$ such that $\gamma(x) = x^3$, for all $x \in \text{GF}(9)$.

$$(A_2, A_3, A_4) = (19794, 428919, 473210)$$

V

Knuth's semifield of type 1 (4 automorphisms) with parameters:

- $k \in \text{GF}(9)$ such that $k^2 + 2k + 2 = 0$;
- $\alpha \in \text{Aut}(\text{GF}(9))$ such that $\alpha(x) = x^3$, for all $x \in \text{GF}(9)$.
- $\beta \in \text{Aut}(\text{GF}(9))$ such that $\beta(x) = x$, for all $x \in \text{GF}(9)$.
- $\gamma \in \text{Aut}(\text{GF}(9))$ such that $\gamma(x) = x^3$, for all $x \in \text{GF}(9)$.

$$(A_2, A_3, A_4) = (19801, 191026, 186259)$$

VI

Knuth's semifield of type 2 (2 automorphisms) with parameters:

- $f \in \text{GF}(9)$ such that $f + 2 = 0$;
- $g \in \text{GF}(9)$ such that $g + 2 = 0$;
- $\sigma \in \text{Aut}(\text{GF}(9))$ such that $\sigma(x) = x^3$, for all $x \in \text{GF}(9)$.

$$(A_2, A_3, A_4) = (19794, 409289, 130416)$$

VII

Knuth's semifield of type 2 (1 automorphism) with parameters:

- $f \in \text{GF}(9)$ such that $f^2 + 2f + 2 = 0$;
- $g \in \text{GF}(9)$ such that $g + 2 = 0$;
- $\sigma \in \text{Aut}(\text{GF}(9))$ such that $\sigma(x) = x^3$, for all $x \in \text{GF}(9)$.

$$(A_2, A_3, A_4) = (19794, 519711, 29089)$$

Besides these 7 known planes, our results showed the existence of 5 new planes:

VIII

Semifield (4 automorphisms) with tuple of matrices

$$(A_2, A_3, A_4) = (19825, 253482, 243782)$$

IX

Semifield (1 automorphism) with tuple of matrices

$$(A_2, A_3, A_4) = (19792, 8841, 198942)$$

X

Semifield (1 automorphism) with tuple of matrices

$$(A_2, A_3, A_4) = (19792, 8956, 202821)$$

XI

Semifield (1 automorphism) with tuple of matrices

$$(A_2, A_3, A_4) = (19792, 8956, 408532)$$

XII

Semifield (1 automorphism) with tuple of matrices

$$(A_2, A_3, A_4) = (19792, 8984, 461005)$$

Matrices are encoded as numbers according to the following rule: the last three columns of a matrix A_i , having a one in the i -th position of the first column, and zeroes everywhere else

$$\begin{pmatrix} a_{11} & a_7 & a_3 \\ a_{10} & a_6 & a_2 \\ a_9 & a_5 & a_1 \\ a_8 & a_4 & a_0 \end{pmatrix}$$

are given as the number $\sum_{i=0}^1 a_i 3^i$. For each of the 12 semifield representatives, we computed the order of the autotopy group, the list of all principal isotopes, and the order of their isomorphism groups. All these data are collected in Table 1.

These results show the existence of 27 nonisomorphic planes. Two of them are commutative: the Desarguesian one (I) and the one coordinatized by Dickson's commutative semifield (III). The total amount of commutative semifields of order 81 is three: the finite field $GF(81)$, Dickson's commutative semifield, and one of its isotopes with matrices $(A_1, A_2, A_3, A_4) = (59293, 19818, 12291, 359225)$. Table 2 contains a summary of our results.

4 Concluding remarks

In this paper we study finite semifields of order 81, with the help of computational tools. We obtain a complete classification of finite semifields of such an order 81 and their planes (Tables 1 and 2). The total amount of these planes is 27. Two of them are commutative (coordinatized by three nonisomorphic commutative finite semifields), approximately half of them (16) were previously unknown.

References

- [1] D.E. Knuth, *Finite semifields and projective planes*, Journal of Algebra **2** (1965), 182-217.
- [2] M. Cordero, G. P. Wene, *A survey of finite semifields*, Discrete Mathematics **208/209** (1999), 125-137.













Plane number	S_3 – orbit	Order of At	S/A sum
I		25600	$\frac{1}{4}$
II		640	$\frac{10}{1}$
III		512	$\frac{12}{1} + \frac{2}{4}$
IV		2048	$\frac{6}{2} + \frac{1}{8}$
V		1024	$\frac{6}{1} + \frac{1}{4}$
VI		128	$\frac{42}{1} + \frac{16}{2}$
VII		64	$\frac{100}{1}$
VIII		256	$\frac{24}{1} + \frac{1}{2} + \frac{2}{4}$
IX		32	$\frac{200}{1}$
X		32	$\frac{200}{1}$
XI		16	$\frac{400}{1}$
XII		64	$\frac{100}{1}$

Table 1: Classification of finite semifields of 81 elements (last five are new)

Number of (commutative) classes	Isomorphism	Isotopy	S_3 -action
Previously known	245 (3)	11 (2)	7 (2)
Actual number	2826 (3)	27 (2)	12 (2)

Table 2: 81-element finite semifields

- [3] M. Hall(Jr.), *The theory of groups*, Macmillan, (1959).
- [4] A. R. Calderbank, P. J. Cameron, W. M. Kantor, J. J. Seidel, \mathbb{Z}_4 -Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets, Proc. London Math. Soc **75** (1997), 436–480.
- [5] W. M. Kantor, M. E. Williams, *Symplectic semifield planes and \mathbb{Z}_4 -linear codes*, Transactions of the American Mathematical Society **356** (2004), 895–938.
- [6] S. González, C. Martínez, I.F. Rúa, *Symplectic Spread based Generalized Kerdock Codes*, Designs, Codes and Cryptography **42 (2)** (2007), 213–226.
- [7] J. P. May, D. Saunders, Z. Wan, *Efficient Matrix Rank Computation with Applications to the Study of Strongly Regular Graphs*, Proceedings of ISSAC 2007, 277-284, ACM, New-York, 2007
- [8] R. J. Walker, *Determination of division algebras with 32 elements*, Proceedings in Symposia of Applied Mathematics **75** (1962), 83-85.
- [9] A. A. Albert, *Finite division algebras and finite planes*, Proceedings of Symposia in Applied Mathematics **10** (1960), 53-70.
- [10] L. E. Dickson, *Linear algebras in which division is always uniquely possible*, Transactions of the American Mathematical Society **7** (1906), 370-390.
- [11] A. A. Albert, *On nonassociative division algebras*, Transactions of the American Mathematical Society **72** (1952), 296-309.
- [12] A. A. Albert, *Finite noncommutative division algebras*, Proceedings of the American Mathematical Society **9** (1958), 928-932.
- [13] A. A. Albert, *Generalized twisted fields*, Pacific Journal of Mathematics **11** (1961), 1-8.
- [14] J. H. M. Wedderburn, *A theorem on finite algebras*, Transactions of the American Mathematical Society **6** (1905), 349–352.
- [15] W. M. Kantor, *Commutative semifields and symplectic spreads*, Journal of Algebra **270** (2003), 96-114.
- [16] I.R. Hentzel, I. F. Rúa, *Primitivity of Finite Semifields with 64 and 81 elements*, International Journal of Algebra and Computation **17 (7)** (2007), 1411-1429.
- [17] G. P. Wene, *On the multiplicative structure of finite division rings*, Aequationes Mathematicae **41** (1991), 222-233.
- [18] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia of mathematics and its applications 20, Addison-Wesley (1983).
- [19] W. M. Kantor, *Finite semifields*, Finite Geometries, Groups, and Computation (Proc. of Conf. at Pingree Park, CO Sept. 2005), de Gruyter, Berlin-New York (2006).

- [20] Menichetti, G. Algebre Tridimensionali su un campo di Galois. Ann. Mat. Pura Appl. **1973**, 97, 293-302.
- [21] Menichetti, G. On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field. Journal of Algebra **1977**, 47, 400-410.